DUMPSHQ

# Free Questions for PCSFE by dumpshq

## Shared by Porter on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

# Question 1

**Question Type:** **MultipleChoice**

Regarding network segmentation, which two steps are involved in the configuration of a default route to an internet router? (Choose two.)

## Options:

**A-** Select the Static Routes tab, then click Add.

**B-** Select Network > Interfaces.

**C-** Select the Config tab. then select New Route from the Security Zone Route drop-down menu.

**D-** Select Network > Virtual Router, then select the default link to open the Virtual Router dialog.

## Answer:

A, D

## Explanation:

To configure a default route to an internet router, you need to select Network > Virtual Router, then select the default link to open the Virtual Router dialog. Then, select the Static Routes tab, then click Add.You can then specify the destination as 0.0.0.0/0 and the next hop as the IP address of the internet router1. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE)

# Question 2

**Question Type: MultipleChoice**

How are CN-Series firewalls licensed?

## Options:

**A-** Data-plane vCPU

**B-** Service-plane vCPU

**C-** Management-plane vCPU

**D-** Control-plane vCPU

## Answer:

A

## Explanation:

CN-Series firewalls are licensed by data-plane vCPU. Data-plane vCPU is the number of virtual CPUs assigned to the data plane of the CN-Series firewall instance. The data plane is the part of the CN-Series firewall that processes network traffic and applies security policies. CN-Series firewalls are licensed by data-plane vCPU, which determines the performance and capacity of the CN-Series firewall instance, such as throughput, sessions, policies, rules, and features. CN-Series firewalls are not licensed by service-plane vCPU, management-plane vCPU, or control-plane vCPU, as those are not factors that affect the licensing cost or consumption of CN-Series firewalls. Reference: [Palo Alto Networks Certified Software Firewall Engineer (PCSFE)], [CN-Series Licensing], [CN-Series System Requirements], [CN-Series Architecture]

# Question 3

**Question Type: MultipleChoice**

What are two requirements for automating service deployment of a VM-Series firewall from an NSX Manager? (Choose two.)

## Options:

**A-** vCenter has been given Palo Alto Networks subscription licenses for VM-Series firewalls.

**B-** Panorama has been configured to recognize both the NSX Manager and vCenter.

**C-** The deployed VM-Series firewall can establish communications with Panorama.

**D-** Panorama can establish communications to the public Palo Alto Networks update servers.

## Answer:

B, C

## Explanation:

The two requirements for automating service deployment of a VM-Series firewall from an NSX Manager are:

Panorama has been configured to recognize both the NSX Manager and vCenter.

The deployed VM-Series firewall can establish communications with Panorama.

NSX Manager is a software component that provides centralized management and control of the NSX environment, including network virtualization, automation, and security. Service deployment is a process that involves deploying and configuring network services, such as firewalls, load balancers, or routers, on the NSX environment. VM-Series firewall is a virtualized version of the Palo Alto Networks next-generation firewall that can be deployed on various cloud or virtualization platforms, including NSX. Panorama is a centralized management server that provides visibility and control over multiple Palo Alto Networks firewalls and devices. Panorama has been configured to recognize both the NSX Manager and vCenter is a requirement for automating service deployment of a VM-Series firewall from an NSX Manager. vCenter is a software component that provides centralized management and control of the VMware environment, including hypervisors, virtual machines, and other resources. Panorama has been configured to recognize both the NSX Manager and vCenter by adding them as VMware service managers and enabling service insertion for VM-Series firewalls on NSX. This allows Panorama to communicate with the NSX Manager and vCenter, retrieve information about the NSX environment, and deploy and manage VM-Series firewalls as network services on the NSX environment. The deployed VM-Series firewall can establish communications with Panorama is a requirement for automating service deployment of a VM-Series firewall from an NSX Manager. The deployed VM-Series firewall can establish communications with Panorama by registering with Panorama using its serial number or IP address, and receiving configuration updates and policy rules from Panorama. This allows the VM-Series firewall to operate as part of the Panorama management domain, synchronize its settings and status with Panorama, and report its logs and statistics to Panorama. vCenter has been given Palo Alto Networks subscription licenses for VM-Series firewalls and Panorama can establish communications to the public Palo Alto Networks update servers are not requirements for automating service deployment of a VM-Series firewall from an NSX Manager, as those are not related or relevant factors for service deployment automation. Reference: [Palo Alto Networks Certified Software Firewall Engineer (PCSFE)], [Deploy the VM-Series Firewall on VMware NSX-T], [Panorama Overview], [VMware Service Manager], [Register the Firewall with Panorama]

# Question 4

**Question Type: MultipleChoice**

Which two routing options are supported by VM-Series? (Choose two.)

## Options:

**A-** OSPF

**B-** RIP

**C-** BGP

**D-** IGRP

## Answer:

A, C

## Explanation:

The two routing options that are supported by VM-Series are:

OSPF

BGP

Routing is a process that determines the best path for sending network packets from a source to a destination. Routing options are protocols or methods that enable routing between different networks or devices. VM-Series firewall is a virtualized version of the Palo Alto Networks next-generation firewall that can be deployed on various cloud or virtualization platforms. VM-Series firewall supports various routing options that allow it to participate in dynamic routing environments and exchange routing information with other routers or devices. OSPF and BGP are two routing options that are supported by VM-Series. OSPF is a routing option that uses link-state routing algorithm to determine the shortest path between routers within an autonomous system (AS). BGP is a routing option that uses path vector routing algorithm to determine the best path between routers across different autonomous systems (ASes). RIP and IGRP are not routing options that are supported by VM-Series, but they are related protocols that can be used for other purposes. Reference: [Palo Alto Networks Certified Software Firewall Engineer (PCSFE)], [VM-Series Deployment Guide], [Routing Overview], [What is OSPF?], [What is BGP?]

## Question 5

**Question Type: MultipleChoice**

Which feature must be configured in an NSX environment to ensure proper operation of a VM-Series firewall in order to secure east-west traffic?

### Options:

**A-** Deployment of the NSX DFW

**B-** VMware Information Sources

**C-** User-ID agent on a Windows domain server

**D-** Device groups within VMware Services Manager

### Answer:

A

### Explanation:

Deployment of the NSX Distributed Firewall (DFW) must be configured in an NSX environment to ensure proper operation of a VM-Series firewall in order to secure east-west traffic. East-west traffic is the traffic that flows between applications or workloads within a network or a cloud environment. NSX environment is a private cloud environment that provides software-defined networking (SDN) and security for heterogeneous endpoints and workloads across multiple hypervisors, containers, bare metal servers, or clouds. NSX DFW is a feature that provides distributed stateful firewalling at the hypervisor level for every virtual machine (VM) in an NSX environment. Deployment of the NSX DFW must be configured in an NSX environment to ensure proper operation of a VM-Series firewall in order to secure east-west traffic by enabling features such as service insertion, policy redirection, service chaining, orchestration, monitoring, logging, and automation for VM-Series firewalls and Panorama on NSX environment. VMware Information Sources, User-ID agent on a Windows domain server, and device groups within VMware Services Manager do not need to be configured in an NSX environment to ensure proper operation of a VM-Series firewall in order to secure east-west traffic, as those are not required or relevant components for NSX integration. Reference: [Palo Alto Networks Certified Software Firewall Engineer (PCSFE)], [Deploy the VM-Series Firewall on VMware NSX-T], [What is VMware NSX-T?], [What is NSX Distributed Firewall?]

# Question 6

**Question Type: MultipleChoice**

What is the structure of the YAML Ain't Markup Language (YAML) file repository?

## Options:

**A-** Deployment Type/Kubernetes/Environment

**B-** Kubernetes/Deployment Type/Environment

**C-** Kubernetes/Environment/Deplovment Type

**D-** Environment/Kubernetes/Deployment Type

## Answer:

B

## Explanation:

Kubernetes/Deployment Type/Environment is the structure of the YAML Ain't Markup Language (YAML) file repository. YAML is a human-readable data serialization language that is commonly used for configuration files. YAML file repository is a collection of YAML files that specify the resources and configuration for deploying and managing infrastructure components, such as firewalls, load balancers, networks, or servers. Kubernetes/Deployment Type/Environment is the structure of the YAML file repository that organizes the YAML files based on the following criteria:

Kubernetes: The platform that provides orchestration, automation, and management of containerized applications.

Deployment Type: The method or model of deploying and managing infrastructure components, such as Terraform, Ansible, Helm, or Kubernetes manifests.

Environment: The type or stage of the cloud or virtualization environment, such as development, testing, staging, or production. Deployment Type/Kubernetes/Environment, Kubernetes/Environment/Deployment Type, and Environment/Kubernetes/Deployment Type are not the structure of the YAML file repository, but they are related ways of organizing YAML files based on different criteria.

Reference: [Palo Alto Networks Certified Software Firewall Engineer (PCSFE)], [What is YAML?], [YAML File Repository]

# Question 7

**Question Type: MultipleChoice**

What helps avoid split brain in active-passive high availability (HA) pair deployment?

## Options:

**A-** Using a standard traffic interface as the HA2 backup

**B-** Enabling preemption on both firewalls in the HA pair

**C-** Using the management interface as the HA1 backup link

**D-** Using a standard traffic interface as the HA3 link

## Answer:

C

### Explanation:

Using the management interface as the HA1 backup link helps avoid split brain in active-passive high availability (HA) pair deployment. High availability (HA) is a feature that provides redundancy and failover protection for firewalls in case of hardware or software failure. Active-passive HA is a mode of HA that consists of two firewalls in a pair, where one firewall is active and handles all traffic, while the other firewall is passive and acts as a backup. Split brain is a condition that occurs when both firewalls in an HA pair assume the active role and start processing traffic independently, resulting in traffic duplication, policy inconsistency, or session disruption. Split brain can be caused by network failures, device failures, or configuration errors that prevent the firewalls from communicating their HA status and synchronizing their configurations and sessions. Using the management interface as the HA1 backup link helps avoid split brain in active-passive HA pair deployment. The HA1 interface is used for exchanging HA state information and configuration synchronization between the firewalls. Using the management interface as the HA1 backup link provides redundancy and failover protection for the HA1 interface, ensuring that the firewalls can maintain their HA communication and avoid split brain. Using a standard traffic interface as the HA2 backup, enabling preemption on both firewalls in the HA pair, or using a standard traffic interface as the HA3 link do not help avoid split brain in active-passive HA pair deployment, but they are related features that can enhance performance and reliability. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [High Availability Overview], [Configure HA Backup Links], [Configure Heartbeat Backup]

# Question 8

**Question Type:** **MultipleChoice**

How does a CN-Series firewall prevent exfiltration?

## Options:

**A-** It employs custom-built signatures based on hash

**B-** It distributes incoming virtual private cloud (VPC) traffic across the pool of VM-Series firewalls.

**C-** It provides a license deactivation API key.

**D-** It inspects outbound traffic content and blocks suspicious activity.

## Answer:

D

## Explanation:

CN-Series firewall prevents exfiltration by inspecting outbound traffic content and blocking suspicious activity. Exfiltration is a technique used by attackers to steal sensitive data or assets from a compromised network or system, usually by sending them to an external destination, such as a command and control server, a drop zone, or an email address. CN-Series firewall is a containerized firewall that integrates with Kubernetes and provides visibility and control over container traffic. CN-Series firewall prevents exfiltration by inspecting outbound traffic content and blocking suspicious activity using threat prevention technologies, such as antivirus, anti-spyware, vulnerability protection, URL filtering, file blocking, data filtering, and WildFire analysis. CN-Series firewall does not prevent exfiltration by employing custom-built signatures based on hash, distributing incoming virtual private cloud (VPC) traffic across the pool of VM-Series firewalls, or providing a license deactivation API key, as those are not valid or relevant methods for exfiltration prevention.

Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [CN-Series Concepts], [CN-Series Deployment Guide for

Native K8], [Threat Prevention Datasheet], [What is Exfiltration?]

# Question 9

**Question Type:** **MultipleChoice**

Which software firewall would assist a prospect who is interested in securing extensive DevOps deployments?

## Options:

**A-** CN-Series

**B-** Ion-Series

**C-** Cloud next-generation firewall

**D-** VM-Series

## Answer:

D

### Explanation:

VM-Series firewall is the software firewall that would assist a prospect who is interested in securing extensive DevOps deployments. DevOps is a set of practices that combines software development and IT operations to deliver software products faster and more reliably. DevOps deployments require network security that can protect the traffic between different stages of the software development lifecycle, such as development, testing, staging, and production, as well as between different cloud or virtualization platforms, such as public clouds, private clouds, or on-premises data centers. VM-Series firewall is a virtualized version of the Palo Alto Networks next-generation firewall that can be deployed on various cloud or virtualization platforms. VM-Series firewall can assist a prospect who is interested in securing extensive DevOps deployments by providing comprehensive security and visibility across hybrid and multi-cloud environments, protecting applications and data from cyberattacks, and supporting automation and orchestration tools that simplify and accelerate the deployment and configuration of firewalls across different platforms. CN-Series, Ion-Series, and Cloud next-generation firewall are not software firewalls that would assist a prospect who is interested in securing extensive DevOps deployments, but they are related solutions that can be deployed on specific platforms or environments. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [VM-Series Datasheet], [VM-Series Deployment Guide], [What is DevOps?]

## Question 10

**Question Type:** MultipleChoice

Which two valid components are used in installation of a VM-Series firewall in an OpenStack environment? (Choose two.)

## Options:

**A-** OpenStack heat template in JSON format

**B-** OpenStack heat template in YAML Ain't Markup Language (YAML) format

**C-** VM-Series VHD image

**D-** VM-Series qcow2 image

## Answer:

B, D

## Explanation:

The two valid components that are used in installation of a VM-Series firewall in an OpenStack environment are:

OpenStack heat template in YAML Ain't Markup Language (YAML) format

VM-Series qcow2 image

OpenStack is a cloud computing platform that provides infrastructure as a service (IaaS) for deploying and managing virtual machines (VMs) and other resources. OpenStack environment requires network security that can protect the traffic between VMs or other cloud services from cyberattacks and enforce granular security policies based on application, user, content, and threat information. VM-Series firewall is a virtualized version of the Palo Alto Networks next-generation firewall that can be deployed on various cloud or virtualization platforms, including OpenStack. OpenStack heat template in YAML format is a valid component that is used in installation of a VM-Series firewall in an OpenStack environment. OpenStack heat template is a file that defines the resources and configuration for deploying and managing a VM-Series firewall instance on OpenStack. YAML is a human-readable data serialization language that is commonly used for configuration files. YAML format is supported for OpenStack heat templates for VM-Series firewalls. VM-Series qcow2 image is a valid component that is used in installation of a VM-Series firewall in an OpenStack environment. VM-Series qcow2 image is a file that contains the software image of the VM-Series firewall for OpenStack. qcow2 is a disk image format that supports features such as compression, encryption, snapshots, and copy-on-write. qcow2 format is supported for VM-Series images for OpenStack. OpenStack heat template in JSON format and VM-Series VHD image are not valid components that are used in installation of a VM-Series firewall in an OpenStack environment, as those are not supported formats for OpenStack heat templates or VM-Series images. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Deploy the VM-Series Firewall on OpenStack], [What is YAML?], [What is qcow2?]

# Question 11

**Question Type:** **MultipleChoice**

Which software firewall would help a prospect interested in securing an environment with Kubernetes?

## Options:

**A-** KN-Series

**B-** ML-Series

**C-** VM-Series

**D-** CN-Series

## Answer:

D

## Explanation:

CN-Series firewall is the software firewall that would help a prospect interested in securing an environment with Kubernetes. Kubernetes is a platform that provides orchestration, automation, and management of containerized applications. Kubernetes environment requires network security that can protect the inter-service communication from cyberattacks and enforce granular security policies based on application or workload characteristics. CN-Series firewall is a containerized firewall that integrates with Kubernetes and provides visibility and control over container traffic. CN-Series firewall can help a prospect interested in securing an environment with Kubernetes by inspecting and enforcing security policies on traffic between containers within a pod, across pods, or across namespaces in a Kubernetes cluster. KN-Series, ML-Series, VM-Series, and Cloud next-generation firewall are not software firewalls that would help a prospect interested in securing an environment with Kubernetes, but they are related solutions that can be deployed on different platforms or environments. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [CN-Series Datasheet], [CN-Series Concepts], [What is Kubernetes?]